

**WILLKIE FARR & GALLAGHER LLP**

BENEDICT HUR (SBN 224018)

bhur@willkie.com

SIMONA AGNOLUCCI (SBN 246943)

sagnolucci@willkie.com

EDUARDO SANTACANA (SBN 281668)

esantacana@willkie.com

DAVID D. DOAK (SBN: 301319)

ddoak@willkie.com

JOSHUA D. ANDERSON (SBN: 312836)

jpanderson@willkie.com

TIFFANY LIN (SBN 321472)

tlin@willkie.com

HARRIS MATEEN (SBN 335593)

hmateen@willkie.com

NAIARA TOKER (SBN 346145)

ntoker@willkie.com

333 Bush Street, 34<sup>th</sup> Floor

San Francisco, California 94104

Telephone: (415) 858-7400

Attorneys for Defendant

**GOOGLE LLC**

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

JANE DOE I, et al., individually and on  
behalf of all others similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No. 3:23-cv-02431-VC  
(Consol. w/ 3:32-cv-02343-VC)

**DEFENDANT GOOGLE LLC'S REPLY  
IN SUPPORT OF ITS MOTION TO  
DISMISS**

**Date: March 14, 2024**

**Time: 10:00 a.m.**

**Ctrm.: 4**

Consol. Complaint Filed: July 13, 2023

*District Judge Vince Chhabria  
San Francisco Courthouse, Ctrm. 4*

## **TABLE OF CONTENTS**

I.	INTRODUCTION .....	1
II.	ARGUMENT .....	1
A.	Plaintiffs’ claims do not satisfy the heightened standard of Rule 9(b) .....	1
B.	Plaintiffs’ wiretap claim should be dismissed (Count 1) .....	2
C.	Plaintiffs’ CIPA claims should be dismissed (Count 2) .....	4
D.	Plaintiffs’ invasion of privacy claims should be dismissed (Counts 3 and 4 ) .....	7
E.	Plaintiffs fail to establish UCL standing and reliance (Count 5) .....	7
F.	Plaintiffs’ trespass to chattels and conversion claims are frivolous (Counts 6 and 12) .....	9
G.	California Comprehensive Data Access and Fraud Act (CDAFA) (Count 7) .....	9
H.	Breach of contract (Count 8) .....	12
I.	Breach of implied contract (Count 9) .....	14
J.	Breach of implied covenant of good faith and fair dealing (Count 10) .....	15
K.	Unjust enrichment (Count 11) .....	15
III.	CONCLUSION .....	15

**TABLE OF AUTHORITIES**

	<b>Page(s)</b>
<b>Cases</b>	
<i>Apumac, LLC v. Flint Hills Int’l</i> , 2015 WL 13306128 (C.D. Cal. Feb. 6, 2015).....	1
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	6
<i>Bass v. Facebook, Inc.</i> , 394 F. Supp. 3d 1024 (N.D. Cal. 2019) .....	8
<i>Brown v. Google LLC</i> , 2021 WL 6064009, at *17 (N.D. Cal. Dec. 22, 2021) .....	7, 8, 11
<i>Brown v. Google LLC</i> , 2023 WL 5029899 (N.D. Cal. Aug. 7, 2023) .....	11
<i>Caraccioli v. Facebook, Inc.</i> , 167 F.Supp.3d 1056 (N.D. Cal. 2016) .....	12
<i>In re Carrier IQ, Inc.</i> , 78 F. Supp. 3d 1051 (N.D. Cal. 2015) .....	10
<i>Cottle v. Plaid Inc.</i> , 536 F. Supp. 3d 461 (N.D. Cal. 2021) .....	9, 11
<i>Doe I v. Google LLC</i> , 2023 WL 6882766 (N.D. Cal. Oct. 18, 2023).....	2, 3, 4
<i>Doe v. Meta Platforms, Inc.</i> , 2023 WL 5837443, *5 (N.D. Cal. Sept. 7, 2023) .....	3, 4
<i>eBay, Inc. v. Bidder's Edge, Inc.</i> , 100 F. Supp. 2d 1058 (N.D. Cal. 2000) .....	9
<i>In re Facebook, Inc. Internet Tracking Litig.</i> , 956 F.3d 589(9th Cir. 2020) .....	6, 11
<i>Facebook, Inc. v. Power Ventures, Inc.</i> , 2010 WL 3291750 (N.D. Cal. July 20, 2010).....	11, 12
<i>Fink v. Time Warner Cable</i> , 2009 WL 2207920 (S.D.N.Y. July 23, 2009) .....	11
<i>In re Google Assistant Privacy Litig.</i> , 457 F. Supp. 3d 787 (N.D. Cal. 2020) .....	13

<i>Gorlach v. Sports Club Co.</i> , 209 Cal. App. 4th 1497 (2012) .....	14
<i>Grace v. Apple Inc.</i> , 2017 WL 3232464, at *11 (N.D. Cal. July 28, 2017).....	9
<i>Graham v. Noom, Inc.</i> , 533 F. Supp. 3d 823 .....	5, 6
<i>Guz v. Bechtel Nat. Inc.</i> , 24 Cal. 4th 317 (2000) .....	15
<i>Hammerling v. Google LLC</i> , 615 F. Supp. 3d 1069 .....	15
<i>In re iPhone Application Litig.</i> , 844 F. Supp. 2d 1040 .....	11
<i>In re: Lenovo Adware Litig.</i> , 2016 WL 6277245 (N.D. Cal. Oct. 27, 2016).....	9
<i>In re Nickelodeon Consumer Priv. Litig.</i> , 827 F.3d 262 (3d Cir. 2016).....	4
<i>In re Pharmatrak, Inc.</i> , 329 F.3d 9 (1st Cir. 2003).....	2, 3
<i>James v. Allstate Ins. Co.</i> , 2023 WL 8879246 (N.D. Cal. Dec. 22, 2023).....	5
<i>Javier v. Assurance IQ, LLC</i> , 2023 WL 114225 (N.D. Cal. Jan. 5, 2023).....	5
<i>Johnson-Jack v. Health-Ade LLC</i> , 587 F. Supp. 3d 957 (N.D. Cal. 2022) .....	2
<i>Katz-Lacabe v. Oracle Am., Inc.</i> , 2023 WL 2838118 (N.D. Cal. Apr. 6, 2023) .....	6, 8
<i>Kearns v. Ford Motor Co.</i> , 567 F.3d 1120 (9th Cir. 2009) .....	2
<i>Kissel v. Code 42 Software, Inc.</i> , 2016 WL 7647691, at *8 (C.D. Cal. Apr. 14, 2016) .....	8
<i>Korea Supply Co. v. Lockheed Martin Corp.</i> , 29 Cal. 4th 1134 (2003) .....	7
<i>Kurowski v. Rush Sys. For Health</i> , 2023 WL 4707184 (N.D. Ill. July 24, 2023).....	3, 9, 13

<i>Kwikset Corp. v. Superior Court</i> , 51 Cal. 4th 310 (2011) .....	8
<i>Lindsay-Stern v. Garamszegi</i> , 2016 WL 11745948 (C.D. Cal. Oct. 13, 2016).....	10, 12
<i>Lopez v. Apple, Inc.</i> , 519 F. Supp. 3d 672 (N.D. Cal. 2021) .....	4
<i>Metzger v. Wells Fargo Bank, N.A.</i> , 2014 WL 1689278 (C.D. Cal. Apr. 28, 2014) .....	14
<i>Meyer v. Cap. All. Grp.</i> , 2017 WL 5138316 (S.D. Cal. Nov. 6, 2017) .....	9
<i>Mintz v. Mark Bartelstein &amp; Assocs. Inc.</i> , 906 F. Supp. 2d 1017, 1032 (C.D. Cal. 2012) .....	11
<i>Moore v. Centrelake Med. Grp., Inc.</i> , 83 Cal. App. 5th 515 (2022), rev. den'd (Dec. 14, 2022) .....	8
<i>Nguyen v. Barnes &amp; Noble Inc.</i> , 763 F.3d 1171 (9th Cir. 2014) .....	7
<i>NovelPoster v. Javitch Canfield Grp.</i> , 140 F. Supp. 3d 954 (N.D. Cal. 2014) .....	10, 12
<i>Planned Parenthood Fed'n of Am., Inc. v. Newman</i> , 51 F.4th 1125, 1136 (9th Cir. 2022) .....	3
<i>Pratt v. Higgins</i> , 2023 WL 4564551 (N.D. Cal. July 17, 2023).....	10
<i>Pruchnicki v. Envision Healthcare Corp.</i> , 845 F. App'x 613 (9th Cir. 2021) .....	8
<i>Revitch v. New Moosejaw, LLC</i> , 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019).....	6
<i>Rodriguez v. Google LLC</i> , 2021 WL 2026726 (N.D. Cal. May 21, 2021).....	<i>passim</i>
<i>S. Cal. Gas Co. v. City of Santa Ana</i> , 336 F.3d 885 (9th Cir. 2003) .....	13
<i>San Miguel v. HP Inc.</i> , 317 F.Supp.3d 1075 (N.D. Cal. 2018) .....	9
<i>Saroya v. Univ. of the Pac.</i> , 503 F. Supp. 3d 986 (N.D. Cal. 2020) .....	15

<i>Smith v. Facebook, Inc.</i> , 262 F. Supp. 3d 943 (N.D. Cal. May 9, 2017).....	13
<i>Soo v. Lorex Corp.</i> , 2020 WL 5408117 (N.D. Cal. Sept. 9, 2020) .....	9
<i>Stanley v. Univ. of S. Cal.</i> , 178 F.3d 1069 (9th Cir. 1999) .....	14, 15
<i>Sun Life Assurance Co. of Can. v. Imperial Premium Fin., LLC</i> , 904 F.3d 1197 (11th Cir. 2018) .....	15
<i>Swallow v. Roberts</i> , 2020 WL 1428231 (Cal. Ct. App. Mar. 24, 2020).....	11
<i>Taus v. Loftus</i> , 40 Cal. 4th 683 (2007) .....	7
<i>United States v. Collazo</i> , 984 F.3d 1308 (9th Cir. 2021) .....	12
<i>United States v. Olson</i> , 856 F.3d 1216 (9th Cir. 2017) .....	12
<i>Weiner v. ARS Nat’l Servs., Inc.</i> , 887 F. Supp. 2d 1029 (S.D. Cal. 2012).....	6
<i>Welter v. Med. Pro. Mut. Ins. Co.</i> , 2023 WL 2988627 (D. Mass. Feb. 23, 2023) .....	11
<i>Wesch v. Yodlee, Inc.</i> , 2021 WL 6206644 (N.D. Cal. July 19, 2021).....	11
<i>Williams v. DDR Media, LLC</i> , 2023 WL 5352896 (N.D. Cal. Aug. 18, 2023) .....	5
<i>Yoon v. Lululemon USA, Inc.</i> , 549 F. Supp. 3d 1073 (C.D. Cal. 2021) .....	7
<i>Zenith Ins. Co. v. O’Connor</i> , 148 Cal. App. 4th 998 (2007) .....	14
<b>Statutes</b>	
18 U.S. Code Section 1030 .....	10
Cal. Bus. & Prof. Code Section 17204 .....	7, 8
Cal. Civ. Code Section 1621 .....	14

Cal Civ. Code Section 1798.91 .....9

Cal. Penal Code Section 631.....5, 7

Cal. Penal Code Section 632.....6

**Other Authorities**

Rule 8.....1, 15

Rule 9(b) .....1, 2, 4

## I. INTRODUCTION

This is just one of the many poorly pleaded class action complaints filed in recent years alleging that a technology company or a technology company’s customer collected sensitive online data in contravention of the defendant’s public commitments not to do so. Like those other complaints, the Court should dispose of Plaintiffs’ claims of fraudulent activity based on nothing more than finger-pointing and pure speculation. As just one example, in a final attempt to get around the fatal and complete lack of personal advertising that their complaint is premised on, Plaintiffs argue, for the first time, that “[a] decision *not* to show Plaintiffs particular ads based on their health status is just as ‘personalized’ a misuse of their data.” Opp. at 22. Plaintiffs’ overreach and wild guesses cannot supplant concrete factual allegations that state a claim for relief. Plaintiffs fail to meet Rule 8’s requirement of a “short and plain statement of the claim showing that the pleader is entitled to relief,” let alone the heightened specificity Rule 9(b) requires here. The Court should grant Google’s motion.

## II. ARGUMENT

### A. Plaintiffs’ claims do not satisfy the heightened standard of Rule 9(b)

Plaintiffs disclaim the strictures of Rule 9(b) because their claims “do not sound in fraud.” Opp. at 4. Yet the crux of their case is that Google violated its own promises to developers and the public, and surreptitiously collected and used sensitive health information for its own gain; at times, Plaintiffs argue that Google acted with a criminal purpose. Plaintiffs’ attempt to avoid the rules is why it is the nature of the allegations, not the *ipse dixit* of a plaintiff, that determines whether a claim “sounds in fraud.” *Apumac, LLC v. Flint Hills Int’l*, 2015 WL 13306128, at \*5 (C.D. Cal. Feb. 6, 2015) (noting that “Rule 9(b) applies to allegations of fraud, not just claims of fraud”).

Plaintiffs’ allegations are substantively indistinguishable from those Judge Seeborg found to require application of Rule 9(b). See *Rodriguez v. Google LLC*, 2021 WL 2026726, at \*6 (N.D. Cal. May 21, 2021). The plaintiffs in *Rodriguez* alleged that Google used “secret scripts” to “surreptitiously” collect online activity through Google Analytics (“GA”) on third-party apps, which allegedly violated representations Google made in its Privacy Policy and elsewhere. *Id.* at \*2–3. Here, Plaintiffs make the same allegations of “disguised” cookies “secretly embedded” through third-party websites, collecting



data Google promises not to collect as part of a “conspir[acy]”. FAC ¶¶ 5, 54, 57, 60(c), 289–302, 440(a) (“Google conspired with Health Care Providers”); Opp. at 7 (“Google’s interception occurs for the illegitimate purposes of compiling protected information.”). Plaintiffs cannot allege “secretly” plotting to mislead users for an “illegitimate purpose” while avoiding Rule 9(b). Because each of Plaintiff’s claims is premised on this alleged “unified course of fraudulent conduct,” each claim is subject to Rule 9(b). *See Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009). And the allegations come nowhere close to meeting their burden to “state with particularity” “‘the who, what, when, where, and how’” *of the circumstances constituting the alleged fraud. Johnson-Jack v. Health-Ade LLC*, 587 F. Supp. 3d 957, 973 (N.D. Cal. 2022) (citations omitted). *See* Opp. at 4 (purportedly laying out the who, what, when, where, and how). As in *Rodriguez*, the FAC is silent on “when the ‘secret scripts’ plot was hatched; which Google departments (let alone employees) were involved; and anything resembling a particular date, time, or place.” *Rodriguez*, 2021 WL 2026726, at \*6.

Plaintiffs’ decision to continue to press inadequate allegations is particularly concerning given this case’s procedural history. When invited to provide all the evidence they had on the central question of this case—whether Google stepped outside its role of servicer and used sensitive health information in violation of Plaintiffs’ privacy rights—Plaintiffs fell short on their motion for preliminary injunction. Now, in opposition to a motion to dismiss, Plaintiffs claim they need not allege facts substantiating their accusations at all. Instead, they provide nothing more than the circular logic that because Google *could* benefit from the data, it *must* be using it. More is required before subjecting a defendant to the burdens, reputational harm, and potential legal prejudice of a full-blown complex litigation.

#### **B. Plaintiffs’ wiretap claim should be dismissed (Count 1)**

One-Party Consent: This Court already ruled in rejecting Plaintiffs’ motion for a preliminary injunction that “the health care providers consented to the use of Google source code.” *Doe I v. Google LLC*, 2023 WL 6882766, at \*2 (N.D. Cal. Oct. 18, 2023). Yet Plaintiffs return with a new spin on consent, and out-of-circuit law. As Plaintiffs note, *Pharmatrak* held that the use of a product is insufficient to infer consent, but there, the defendant assured the provider that its service was incapable of collecting PII. *In re Pharmatrak, Inc.*, 329 F.3d 9, 20 (1st Cir. 2003). The court distinguished cases

like this one, where consent was obvious, since the products were acquired for the complained-of purpose, or the purpose was “announced” or “self-evident.” *Id.* In *Doe v. Meta Platforms, Inc.*, Judge Orrick recognized the distinction in *Pharmtrak* but held that the facts alleged in that case were closer to the former category, *as to Meta*. 2023 WL 5837443, \*5 (N.D. Cal. Sept. 7, 2023). Here, as this Court acknowledged at the preliminary injunction hearing, Plaintiffs’ allegations fall in the latter category.

Plaintiffs argue that Google: (1) makes its products available for third parties to “copy-and-paste” into their source code and that the “primary purpose” is to obtain information about users’ communications; (2) discloses the analytics and advertising purposes of the technologies; and (3) “encourages” providers to use its products to collect and use health information. *See* FAC ¶¶ at 40–45, 306. Further, the providers’ intent to collect this data is key to Plaintiffs’ privacy claims. *See* FAC ¶ 440(a) (“Google’s conduct was highly offensive because ... Google conspired with Health Care Providers to violate a cardinal rule of the provider-patient relationship.”). Indeed, these same Plaintiffs’ lawyers *sued healthcare providers* alleging they intentionally violated the same users’ privacy rights by using Google’s products. *See Kurowski v. Rush Sys. For Health*, 2023 WL 4707184, at \*3 (N.D. Ill. July 24, 2023). And contrary to *Doe v. Meta*, the judicially noticeable documents here also show that Google unequivocally informs healthcare providers of the “practice at issue” (Opp. at 5), forbidding healthcare providers from incorporating GA on HIPAA-covered pages. RJN Ex. 2, *HIPAA and Google Analytics*. Plaintiffs cannot claim the providers intended to use Google’s products to collect their data while claiming the providers have no idea the collection was occurring.

Tortious Purpose Exception: Plaintiffs make the same failed tortious purpose argument that has led to various dismissals in this Court. Opp. at 7. The supposed torts are premised on the *same* alleged interception, and do not vitiate consent. *Doe I v. Google LLC*, 2023 WL 6882766, at \*2 (citing *Sussman v. Am. Broad. Companies, Inc.*, 186 F.3d 1200, 1202 (9th Cir. 1999)) (“It is not enough for the interception itself to have violated the law, the interception must be ‘done for the purpose of facilitating some further impropriety.’”). Plaintiffs’ own authorities work against them. In *Planned Parenthood Fed’n of Am., Inc. v. Newman*, the Ninth Circuit held the crime or tort exception did not apply because the purpose of the recording was the same as the purpose of the criminal or tortious act. 51 F.4th 1125, 1136

(9th Cir. 2022) (“§ 2511(2)(d) requires that the criminal or tortious *purpose* be independent of and separate from the *purpose* of the recording.”) (emphasis added). And besides, the purpose alleged is plainly not criminal or tortious. *Rodriguez*, 2021 WL 2026726 at \*6 n.8 (Google’s “purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money.”).

Intent: Plaintiffs do not back up their assertions of intent with plausible allegations. Plaintiffs argue that because Google is the “designer and creator” of the products at issue and keeps the data on its servers for developers to use, that means Google “was well aware the interception was occurring.” *See* Opp. at 7. If that were good enough to allege intent, every cloud service provider would be charged with the vicarious intent of anyone who misuses their service. Products that can be used for legal and illegal purposes do not subject the manufacturer to vicarious liability for the product’s every use, especially here where the vast majority of developers use Google’s products in an indisputably legitimate manner.<sup>1</sup>

Plaintiffs argue that their claims should proceed based on a single sentence of Judge Orrick’s opinion in *Doe v. Meta*, which concluded without analysis that “[w]hat Meta’s true intent is, [and] what steps it actually took to prevent receipt of health information ... turn on disputed questions of fact that need development on a full evidentiary record.” *Doe v. Meta*, 2023 WL 5837443, \* 3. But Judge Orrick relied solely on *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 684 (N.D. Cal. 2021), a case that did not contain any public policies prohibiting the very practice that plaintiffs complained of. *Id.* Judge Orrick was not asked to consider whether allegations that a defendant intended that its own policies be violated, as alleged here, must satisfy Rule 9(b). A mere assertion is not enough. *Rodriguez*, 2021 WL 2026726, at \*6 (allegations of Google’s “secret scripts” “must be accompanied by ‘the who, what, when, where, and how’ of the misconduct charged”). To allege that Google prohibits websites from sending it PII and PHI, but nevertheless intended that the websites would violate the prohibition so that it could monetize PII and PHI is a salacious allegation that must be supported by Rule 9(b) particularity.

### **C. Plaintiffs’ CIPA claims should be dismissed (Count 2)**

Vendor: A vendor who provides a tool for a website to record user interactions cannot be liable

---

<sup>1</sup> *See e.g., Doe I v. Google LLC*, 2023 WL 6882766, at \*2 (finding it is possible, based on the evidence presented, that Google is merely a vendor providing the GA service); *see also In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 294 (3d Cir. 2016) (“courts have long understood that tracking cookies can serve legitimate commercial purposes.”).

for the recording. *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 833. Most courts key off of California case law that distinguishes the manufacturer of a tape recorder from a secret listener. *See Williams v. DDR Media, LLC*, 2023 WL 5352896, at \*4 (N.D. Cal. Aug. 18, 2023) (noting that “whether [defendant’s] software is more akin to a tape recorder or a secret listener ... is a close question, and district courts have split on the issue.”). Various judges have already agreed with *Noom* in circumstances like this one, where use of the data has not adequately been alleged. *See* MTD at 9–10 (citing *Williams v. What If Holdings*, 2022 WL 17869275, at \*3; *Johnson v. Blue Nile, Inc.*, 2021 WL 1312771, at \*3 (N.D. Cal. Apr. 8, 2021); *Yale v. Clicktale, Inc.*, 2021 WL 1428400, at \*3 (N.D. Cal. Apr. 15, 2021)).

Judge Breyer’s dicta in *Javier v. Assurance IQ, LLC*, 2023 WL 114225, at \*5 (N.D. Cal. Jan. 5, 2023), can easily be reconciled with this line of cases. There, Judge Breyer noted that if the tool’s provider “does not have the capability to use its record of the interaction for any other purpose,” liability will not lie; but if the tool has “the *capability* to use its record of the interaction for any other purpose,” the tool’s provider could be liable. *Id.* at \*6 (emphasis added). A focus on the tool’s other capabilities is misplaced, because the second clause of section 631(a) “penalizes anyone who ‘reads, or attempts to read, or to learn the contents or meaning of’ the communication,” and does not cover a software company that “merely recorded the communication for retrieval by a party to the same communication.” *DDR Media, LLC*, 2023 WL 5352896, at \*4 (quoting Cal. Penal Code § 631(a) and concluding that *Javier* and *Ribas v. Clark*, 38 Cal. 3d 355 (1985) are inapplicable to the second prong); *see also James v. Allstate Ins. Co.*, 2023 WL 8879246, at \*3 (N.D. Cal. Dec. 22, 2023) (“[A]llegation that ‘this data is stored or can be accessed by Heap’ is insufficient to support a plausible inference Heap attempted to read or learn the contents of the communication while in transit.”).

But in a case like this, Plaintiffs cannot distinguish the *Noom* line of cases by arguing Google acquires information for its own purposes (an argument unrelated to the *capability* of the tool). Opp. at 9. The allegations make clear that the “purposes” in question are the purposes of the Websites, and that the tool requires both the website and users to take action that Plaintiffs never allege has occurred here. *See e.g.* FAC ¶¶ 127, 163, 168, 181 (advertisers must incorporate conversion tracking, link their Ads and Analytics accounts to enable data to flow between them, enable remarketing, and activate Signals), 183–

84 (users must have consented to association of data in My Activity and enable Ads Personalization).

At bottom, Plaintiffs are asking this Court to conclude that because Google *could have* marketing or advertising capabilities, it *must have* used those features here with the Websites’ data in an unlawful manner. This is precisely the type of speculative pleading that is impermissible. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (“Where a complaint pleads facts that are ‘merely consistent with’ a defendant’s liability, it ‘stops short of the line between possibility and plausibility of ‘entitlement to relief’”) (cleaned up). This distinguishes Plaintiffs’ allegations from the cases they rely on. *See* Opp. at 9; *Noom*, 533 F. Supp. 3d at 832 (distinguishing *In re Facebook, Inc.* as that case contained allegations that vendor independently mined and sold information); *Katz-Lacabe v. Oracle Am., Inc.*, 2023 WL 2838118, at \* 1–2, 9 n.8 (N.D. Cal. Apr. 6, 2023) (alleging “Oracle combines and sells information”).

CIPA Section 632: Plaintiffs’ section 632 claim fails on a plain reading of the statutory text, which penalizes a *defendant who records* a confidential communication. *See* Cal. Penal Code § 632; *Weiner v. ARS Nat’l Servs., Inc.*, 887 F. Supp. 2d 1029, 1032 (S.D. Cal. 2012); *see also Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at \*3 (N.D. Cal. Oct. 23, 2019) (“Section 632 ‘does not prohibit eavesdropping in general; it applies only to the use of ‘any electronic amplifying or recording device’ to eavesdrop upon or record a confidential communication.’”) (quotations omitted). Plaintiffs’ opposition makes clear that their section 632 claim is really a section 631 claim. *See* Opp. at 10 (Google “ignores Plaintiffs’ allegations that Google, via its Source Code, ... *intercepts* confidential patient communications *by redirecting this content* to its servers.”) (emphasis added).

Additionally, Plaintiffs point to Google’s “express promises to collect only health information users chose to provide.” Aside from confusing the term “Health Information” as defined by Plaintiffs and by Google in its privacy policy, Plaintiffs also ignore that even an “‘objectively reasonable expectation’ that their communications with third-party apps would not be ‘recorded’ by Google ... does not reasonably give rise to the expectation that *nobody* (including the websites’ developers) would record the communications. To show the latter, plaintiffs must plead unique, definite circumstances rebutting California’s presumption against online confidentiality.” *Rodriguez*, 2021 WL 2026726, at \*7. Put more simply, when a user surfs the web, and the website invites them to accept cookies and tells

them certain information will be recorded, the user can hardly claim that she expected the browsing to be confidential, at least as to the website developer and its technology service provider. Plaintiffs' reliance on *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1178- 79 (9th Cir. 2014) and *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021) misses the dispositive factor in those cases, which addressed whether the mere presence of terms of use or privacy policies can constitute assent to those terms; those cases say nothing about the user's reasonable confidentiality expectations.

Intent: In any event, as criminal statutes, Cal. Penal Code Sections 631 and 632 require intentional conduct. Cal. Penal Code §§ 631(a) (prohibiting "intentional[] tap[ping]"), 632 (making liable a person who "intentionally" records a confidential communication). Plaintiffs do not assert plausible intent allegations, which is fatal to their CIPA claims. *See supra* section II.B.

**D. Plaintiffs' invasion of privacy claims should be dismissed (Counts 3 and 4 )**

Plaintiffs do not remedy their failure to state a plausible invasion of privacy claim. Intrusion upon seclusion is an intentional tort and failure to plausibly allege intent is fatal to the claim. *Taus v. Loftus*, 40 Cal. 4th 683, 725 (2007). Plaintiffs concede Google prohibits the collection they allege, but rely on conclusory allegations that "Google's conduct is knowing and intentional" because Google knows it is collecting Health Information as "Google can readily identify the web properties which use the Google Source Code" and "can easily ... identify the web properties that are Health Care Providers." FAC ¶¶ 204–24. But there are no allegations, for example, that Google instructed the Websites to send sensitive health information. Putting aside that such pleading is insufficient to show intent (*see supra* section II.B), Plaintiffs' theory sounds in fraud—that, despite Google's express statement that it does not want to receive sensitive health data, Google secretly intended to receive such data anyways. Such a theory must be pleaded with particularity. *See Rodriguez*, 2021 WL 2026726, at \*3 .

**E. Plaintiffs fail to establish UCL standing and reliance (Count 5)**

Standing: Contrary to Plaintiffs' allegations (FAC ¶ 373), the UCL requires by its own terms a showing of loss, and does not recognize a right to disgorgement of profits. Cal. Bus. & Prof. Code § 17204; *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1147 (2003). Plaintiffs wrongly continue to rely on a handful of cases, including *Brown* and *Calhoun*, contending that loss of



“information” is enough. “The weight of the authority in the district and the state . . . *point in the opposite direction* [of *Calhoun*]: that the mere misappropriation of personal information does not establish compensable damages.” *Katz-Lacabe*, 2023 WL 2838118, at \*8 (dismissing UCL claim for lack of standing) (emphasis added) (citations omitted); *Rodriguez*, 2021 WL 2026726 at \*8 (“no federal court has wedged individual digital data into the UCL’s ‘money or property’ box”). Plaintiffs’ argument that they establish standing simply by alleging that their personal information was lost fails.<sup>2</sup> *See* Opp. at 12. And, the Ninth Circuit has since held that the external value of data does not show the plaintiff suffered loss. *Pruchnicki v. Envision Healthcare Corp.*, 845 F. App’x 613, 614–15 (9th Cir. 2021).

Further, despite referencing a purported “market” for health data (FAC ¶ 374), Plaintiffs do not adequately allege that this information has value *to them*. “It is not enough to merely say the information was taken and therefore it has lost value . . . . That the information has external value, but no economic value to plaintiff, cannot serve to establish that plaintiff has personally lost money or property.” *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1040 (N.D. Cal. 2019) (dismissing UCL for lack of standing). Moreover, any argument that Plaintiffs could have sold their “medical information” is nonsensical given their alleged privacy concerns over that information. *See Moore v. Centrelake Med. Grp., Inc.*, 83 Cal. App. 5th 515, 538 (2022), rev. den’d (Dec. 14, 2022) (dismissing UCL claim where plaintiffs failed to allege “they ever . . . intended to participate in this market, or . . . derive economic value from their PII.”).

Reliance: Plaintiffs’ allegations and authorities establish that their UCL claim requires reliance. In *Kissel v. Code 42 Software, Inc.*, the court noted that “[w]here a UCL claim sounds in fraud, regardless of the specific UCL prong invoked by the plaintiff, the ‘as a result of’ language ‘imposes an actual reliance requirement.’” 2016 WL 7647691, at \*8 (C.D. Cal. Apr. 14, 2016) (quotations omitted). Here, Plaintiffs base their UCL unlawful claim on statutory and common law violations that sound in fraud. FAC ¶ 462(a)–(b). *See supra* section II.A. Nor does Google “concede[] that the predicate

---

<sup>2</sup> In *Brown*, Judge Koh re-affirmed her decision in *Calhoun*, holding “there is no precedent which suggests that ‘economic injury’ has a different meaning in the UCL context than it does in the Article III context.” 2021 WL 6064009, at \*17 (N.D. Cal. Dec. 22, 2021). But the UCL does not use the term “economic injury”—it uses the phrase “lost money or property.” Cal. Bus. & Prof. Code §17204. That was the type of “economic injury” *Kwikset* reviewed. *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 324 (2011) (“Notably, lost money or property—economic injury—is itself a classic form of injury.”).

violations under the HIPAA, CMIA, CCPA, Cal Civ. Code § 1798.91 to the UCL unlawful claim ... are adequately alleged.” Opp. at 13. There are numerous facial inadequacies with these alleged violations.<sup>3</sup>

**F. Plaintiffs’ trespass to chattels and conversion claims are frivolous (Counts 6 and 12)**

Trespass: Plaintiffs’ theory underlying their trespass claim that Google lodge cookies on Plaintiffs’ computing devices, which resulted in the collection of data, reduced storage, and some unidentified impairment of the devices’ value and functionality has been flatly rejected. *See* MTD at 16–17. Plaintiffs cite readily distinguishable cases to support injury. The trespass in *Grace v. Apple Inc.* disabled video-call functionality on iPhones, which the court distinguished from the mere consumption of memory. 2017 WL 3232464, at \*11 (N.D. Cal. July 28, 2017). Plaintiffs’ remaining authorities are likewise distinguishable as they involve actual loss of function. *Soo v. Lorex Corp.*, 2020 WL 5408117, at \*1, 9 (N.D. Cal. Sept. 9, 2020) (trespass rendered cameras non-functional); *In re: Lenovo Adware Litig.*, 2016 WL 6277245, at \*9 (N.D. Cal. Oct. 27, 2016) (trespass decreased battery life, caused the computers to run slow, blocked or slowed connections to certain websites, and caused security issues); *San Miguel v. HP Inc.*, 317 F.Supp.3d 1075, 1088 (N.D. Cal. 2018) (trespass disabled printers); *eBay, Inc. v. Bidder’s Edge, Inc.*, 100 F. Supp. 2d 1058, 1071–72 (N.D. Cal. 2000) (repetition of the at issue conduct would harm the websites’ systems). Moreover, creating a technology and making it available to anyone who can copy and paste it, *see* FAC ¶ 40, cannot support an “intent” to trespass.

Conversion: Because “[c]onversion requires a higher showing than trespass, it follows that if Plaintiffs have failed to allege a trespass claim, they have also failed to allege a conversion claim. *Meyer v. Cap. All. Grp.*, 2017 WL 5138316, at \*9 (S.D. Cal. Nov. 6, 2017) (citations omitted).

**G. California Comprehensive Data Access and Fraud Act (CDAFA) (Count 7)**

Standing: Plaintiffs’ allegations are indistinguishable from those made in *Kurowski*, wherein the court found no “injury to or interference with” the plaintiff’s devices where the plaintiffs alleged the collection of data “in complete and utter secrecy.” 2023 WL 4707184, at \*10. While true that *Kurowski* was not interpreting CDAFA, *Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461 (N.D. Cal. 2021), confirms that Plaintiffs’ inability to use their devices theory is precluded. There, the court rejected a theory of loss or

---

<sup>3</sup> As just one example, Google—which does not enter into BAA agreements in connection with the relevant services—is not subject to HIPAA.



damage under CDAFA based on the “loss of the right to control their own data, the loss of the value of their data, and the loss of the right to protection of the data,” as that type of loss was not covered by the statute. *Id.* at 488 (citations omitted). Plaintiffs’ cited cases based standing on the “systemic” impact on users’ devices, including slow performance and reduced battery, and on the extended unavailability of the data—none of which is alleged here. *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1056, 1067 (N.D. Cal. 2015); *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 954, 961 (N.D. Cal. 2014).

Plaintiffs next cite a case holding that “emotional damages” are cognizable under CDAFA in order to say their damaged relationships with providers support standing. *Lindsay-Stern v. Garamszegi*, 2016 WL 11745948, at \*6 (C.D. Cal. Oct. 13, 2016); *Opp.* at 17. But, Plaintiffs have not alleged “emotional damages.” And even if they had, *Lindsay-Stern* was incorrect because it conflated standing with remedies. Despite arguing that Google’s reliance on cases interpreting the federal Computer Fraud and Abuse Act (“CFAA”) is misplaced because the definitions of “damage” and “loss” are narrower than those in CDAFA, *Opp.* at 19, Plaintiffs’ authorities make clear that courts apply the definitions of “damage” and “loss” found in the CFAA. *Id.* “Damage” means “impairment to the integrity or availability of data, a program, a system, or information” and “loss” means “any reasonable cost to any victim[.]” 18 U.S.C. § 1030(e)(8), (11). Standing thus requires impairment or actual loss. *See id.* Nevertheless, *Lindsay-Stern* found “emotional damages” support standing because CDAFA allows recovery of “compensatory damages,” which could include “emotional damages.” *Id.* This erroneously conflates the defined term “damage” with the general concept of legal damages. *See* 18 U.S.C. § 1030(g). For CDAFA’s standing limitation to have any force, it must require some actual harm before “emotional damages” may be sought. *See also Pratt v. Higgins*, 2023 WL 4564551, at \*9 (N.D. Cal. July 17, 2023) (accessing medical information gave rise to no cognizable loss under CDAFA).

Plaintiffs also argue that they incurred “expenditures” in responding to the alleged cookies, but such expenditures are nowhere referenced in the Complaint, and the allegations that exist show the absence of a compensable investigation. *See, e.g.,* FAC ¶¶ 518(a) (plaintiffs have been injured through “[t]he expenditure of time and resources to investigate Google’s conduct, including the expenditure of time and resources to retain counsel...” (emphasis added), 20–31 (referencing investigations without

referencing expenditures incurred). Plaintiffs cite *Facebook, Inc. v. Power Ventures, Inc.*, 2010 WL 3291750 (N.D. Cal. July 20, 2010), for the proposition that a “few clicks of a mouse” and “keystrokes” support standing. Setting aside that Plaintiffs do not allege even that much, that court found standing because the plaintiff had to implement technical safeguards to stop the defendant’s access. *Id.* at \*5. Similarly, the plaintiff in *Mintz v. Mark Bartelstein & Assocs. Inc.* had to spend time resetting his password and personally investigating a hacking incident, none of which is alleged here. 906 F. Supp. 2d 1017, 1032 (C.D. Cal. 2012). In *Swallow*, an unpublished California Courts of Appeal decision with no precedential value, plaintiff “testified that he devoted time and effort to determining what data [defendant] accessed.” *Swallow v. Roberts*, 2020 WL 1428231, at \*17 (Cal. Ct. App. Mar. 24, 2020). No such allegations exist here. Attorneys’ fees are also outside the scope of cognizable loss. *Welter v. Med. Pro. Mut. Ins. Co.*, 2023 WL 2988627, at \*10 (D. Mass. Feb. 23, 2023).

Plaintiffs next claim the diminution of value constitutes “damage or loss,” citing *Facebook Tracking* and *Brown v. Google LLC*, 2023 WL 5029899, at \*19 (N.D. Cal. Aug. 7, 2023). However, *Facebook Tracking* analyzed Article III standing, and *Brown* improperly brushed this distinction aside. *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 599–601(9th Cir. 2020). In the related UCL context, a benefit to the defendant only constitute a “loss” to the plaintiff if the plaintiff alleges a market for the data that the plaintiff was willing to participate in, which Plaintiffs do not establish. *See Cottle*, 536 F. Supp. 3d at 484; *Wesch v. Yodlee, Inc.*, 2021 WL 6206644, at \*5 (N.D. Cal. July 19, 2021).

Finally, Plaintiffs argue that “[s]ome impairment resulting from Google’s co-opting of Plaintiffs’ devices is plausible, even if it was not visible to the ordinary consumer.” *Opp.* at 18. Plaintiffs cite no authority for this, instead relying on a “broad conception of ‘damage or loss’ for CDAFA standing.” *Id.* at 19. But, contrary to Plaintiffs’ unfounded assertion, *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040 and the cases cited therein do not turn on the \$5,000 statutory threshold in the CFAA; they turn on plaintiffs’ insufficient and conclusory allegations that fail to establish *any* damage. *Id.*, citing *Bose v. Interclick, Inc.*, 2011 WL 4343517, at \*4, (S.D.N.Y. Aug. 17, 2011) (Plaintiff “fail[ed] to quantify any damage that Interclick caused to her “computers, systems or data that could require economic remedy”); *Fink v. Time Warner Cable*, 2009 WL 2207920, \*4 (S.D.N.Y. July 23, 2009) (dismissing CFAA claim

because Plaintiff’s allegation of impairment to the integrity or availability of data was *insufficiently factual* to frame plausibly the damages element of a CFAA claim) (emphasis added). As noted above, Plaintiffs’ own authorities make clear that courts apply the definitions of “damage” and “loss” in the CFAA to CDAFA. *Lindsay-Stern v. Garamszegi*, 2016 WL 11745948, at \*6, citing *NovelPoster*, 140 F. Supp. 3d at 951 and *Power Ventures*, 2010 WL 3291750, at \*8 (“courts in this circuit have applied the CFAA definitions of ‘loss’ and ‘damage’ to the CDAFA”).

Scienter: Plaintiffs claim they need not allege that Google was aware it acted without authorization. Opp. at 19. But where, as here, a penal statute introduces its elements with “knowingly,” the scienter presumptively applies to all elements. *United States v. Olson*, 856 F.3d 1216, 1220 (9th Cir. 2017). Plaintiffs assert that the Ninth Circuit rejected this presumption for “statutes with grammatical construction of the CDAFA.” Opp. at 19. Not so. The Ninth Circuit continues to hold that “[it] recognizes the presumption . . . that ‘Congress intends to require a defendant to possess a culpable mental state regarding each of the statutory elements that criminalize otherwise innocent conduct.’” *United States v. Collazo*, 984 F.3d 1308, 1324 (9th Cir. 2021).

## **H. Breach of contract (Count 8)**

Breach One: Plaintiffs claim Google’s TOS promise that *other* users must comply with all laws, respect privacy, and refrain from bad behavior. Opp. at 20. That is not what the TOS says. The section titled “What we expect from you” says “you”—not “other users”—“must follow these basic rules of conduct.” Dkt. 86-41 at 5. This is a promise made by Plaintiffs, not Google. Nothing in the agreement suggests Google undertook to become a global law enforcer. See *id.* at 5 (“*If we act on a report of abuse . . .*”) (emphasis added); *Caraccioli v. Facebook, Inc.*, 167 F.Supp.3d 1056, 1064 (N.D. Cal. 2016) (rejecting a similar argument that Facebook’s terms amount to a representation that it will monitor third party content and explaining that the terms impose an obligation on the user, not Facebook).

Breach Two: Plaintiffs claim that the scope of “health information” covered by Google’s Privacy Policy is ambiguous and requires resolution of fact disputes. Opp. at 21. Not so. Google’s Privacy Policy defines health information as “your medical history, vital signs and health metrics (like blood glucose levels), and other similar information related to your physical and mental health.” Dkt. 86-42 at 19. On

its face, this language does not encompass all conceivably health-related information, such as event metadata concerning Plaintiffs’ activity on healthcare websites. It refers to actual medical history or metrics about the specific user. Plaintiffs’ interpretation of this language reads the limiting term “similar” right out of the Privacy Policy.

Plaintiffs wrongly claim they have alleged the collection of actual medical history information. Plaintiffs explanation of the “Health Information” allegedly collected illustrates that it constitutes their internet activity. *Id.* ¶¶ 20–36. This is not the medical history encompassed by Google’s Privacy Policy. *See Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 954–55 (N.D. Cal. May 9, 2017) (health-related internet activity data not PHI); *Kurowski*, 2023 WL 4707184, at \*4 (browsing metadata on healthcare provider’s website “does not in the least bit fit” into the category of individually identifiable health information). Plaintiffs seek to distinguish *Smith* on the basis that the class was not “limited to” patients and the relevant websites were not “limited to” HIPAA-covered entities or involve a similar policy. Opp. at 22. These differences do not impact that court’s conclusion about the nature of the subject data, which equally involved data regarding specific doctors, treatments, and conditions. *Smith*, 262 F. Supp. 3d at 954–55. And, *Kurowski* involved the very same class, entities, and alleged data at issue here.

Plaintiffs do not dispute that Google’s Privacy Policy discloses that it collects internet activity information, or that it identifies controls governing such collection. They argue, however, that the Court should disregard these because the “specific” term governing health information prevails over the “general” terms about web activity. Opp. at 21. Plaintiffs omit that this canon of interpretation only applies when the terms conflict. *S. Cal. Gas Co. v. City of Santa Ana*, 336 F.3d 885, 892 (9th Cir. 2003). Plaintiffs do not identify a conflict, and *Smith* and *Kurowski* show there is none. Plaintiffs cannot state a claim by ignoring the rest of the Privacy Policy. *See In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 787, 832–33 (N.D. Cal. 2020) (dismissing claim that Google breached Privacy Policy by sharing data without consent where Plaintiffs failed to address other circumstances enabling Google to share data).

Breach Three: Plaintiffs baldly assert that “Google’s argument about whether Plaintiffs *received* offending advertisements raises fact questions that are not even relevant to this breach, which concerns Google’s use of Plaintiffs’ Health Information.” Opp. at 22. But Plaintiffs make no effort to identify

even a single allegation that *they* received a personalized advertisement based on *their* health data. This failure is unsurprising. The Complaint itself identifies the settings that both the advertisers and the plaintiffs must enable in order to make their claim remotely possible. This includes advertisers linking analytics and ads accounts and activating Signals, and users enabling relevant My Activity and Ads Personalization controls. FAC ¶¶ 162–68, 181, 183, 184. Plaintiffs do not allege any of this occurred.

Breach Four: Google’s arguments in its opening papers address exactly the portion of the Privacy Policy that Plaintiffs quote from in the FAC. MTD at 23. Plaintiffs assert that Google promised to “use[] the information shared by sites and apps to ... protect against fraud and abuse[.]” ¶ 288, Ex. 51; Opp. at 22. But Plaintiffs continue to manipulate the Privacy Policy by selectively following some hyperlinks but not others. The section Plaintiffs quote from in the FAC and Opposition is immediately followed by an explanatory note and hyperlink: “See our Privacy Policy to learn more about how we process data for each of these purposes.” FAC Ex. 51 at 2. In turn, the hyperlinked privacy policy contains a section describing the use of information to protect against fraud and abuse, which is exactly the portion that Google quotes in its opening papers. MTD at 23, citing RJN Ex. 3 at 18. *See also* FAC Ex. 42 at 18.

#### **I. Breach of implied contract (Count 9)**

An implied contract is created by conduct, not words. Cal. Civ. Code § 1621; *Stanley v. Univ. of S. Cal.*, 178 F.3d 1069, 1078 (9th Cir. 1999). Plaintiffs have not identified what conduct—not words—created an implied contract. The Opposition merely incants the word “conduct” before pointing to words (“Google’s conduct in posting the alleged promises”). Opp. at 23. Aside from this, Plaintiffs identify their own expectations and various laws to support their claim. *Id.* But neither unilateral expectations nor statutes create an implied contract. *See Zenith Ins. Co. v. O’Connor*, 148 Cal. App. 4th 998, 1010 (2007) (plaintiff did not adequately allege implied contract based on subjective belief); *Metzger v. Wells Fargo Bank, N.A.*, 2014 WL 1689278, at \*7 (C.D. Cal. Apr. 28, 2014) (“[A]n implied covenant is based on the terms of the contract, rather than ‘statutory duties imposed.’”). The objective reasonableness of Plaintiffs’ unilateral expectations is irrelevant; it does not show mutual agreement and intent. *Gorlach v. Sports Club Co.*, 209 Cal. App. 4th 1497, 1508 (2012). In fact, Plaintiffs’ assertion that Google “encourages” providers to violate their rights negates any assertion of mutual intent. FAC ¶ 306.

Plaintiffs claim their implied contract claim is not duplicative because they allege the very same promises and breaches in the alternative, in case the TOS and Privacy Policy are not an “express contract.” Opp. at 23; FAC ¶ 546. But an implied contract is a distinct species of contract, not a second bite at the apple when an express contract is not enforceable. Because Plaintiffs base their claim on Google’s *words*, they must bring an express contract claim or none at all. *See Stanley*, 178 F.3d at 1078; *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1095–96.

**J. Breach of implied covenant of good faith and fair dealing (Count 10)**

Plaintiffs’ explanation of their implied covenant claim makes no sense. Plaintiffs state, without any authority, that Google breached the covenant “by drafting and selectively interpreting its contracts” in a specific manner. Opp. at 24. But the covenant of good faith and fair dealing “cannot impose substantive duties or limits on the contracting parties beyond those incorporated in the specific terms of their agreement.” *Guz v. Bechtel Nat. Inc.*, 24 Cal. 4th 317, 349–50 (2000). There is no authority that imposes a covenant of good faith and fair dealing in the *drafting* of the contract. That would patently undermine the freedom of contracting parties to pursue their individual self-interest. Perhaps the argument that Google “abused its power” in drafting sounds in unconscionability. But the invalidity of Google’s TOS and Privacy Policy also invalidates Plaintiffs’ contract claims. Plaintiffs cannot have it both ways, and in neither case have Plaintiffs stated a valid implied covenant claim.

**K. Unjust enrichment (Count 11)**

Unjust enrichment is unavailable where a contract governs “unless the plaintiff also pleads facts suggesting that the contract may be unenforceable or invalid.” *Saroya v. Univ. of the Pac.*, 503 F. Supp. 3d 986, 998 (N.D. Cal. 2020). While true that Plaintiffs were free to plead an unjust enrichment theory in the alternative, Opp. at 25, they did not do so. “Rule 8(d)(2) requires that ‘alternative statements’ be ‘set out’ in the pleading, a requirement that is generally met through ‘either-or’ propositions’ or ‘if-then’ allegations.” *Sun Life Assurance Co. of Can. v. Imperial Premium Fin., LLC*, 904 F.3d 1197, 1213 (11th Cir. 2018) (citations omitted).

### III. CONCLUSION

Google respectfully requests that the Court dismiss Plaintiffs’ Complaint in its entirety.

Dated: February 8, 2024

WILLKIE FARR & GALLAGHER LLP  
Benedict Hur  
Simona Agnolucci  
Eduardo Santacana  
David Doak  
Joshua Anderson  
Tiffany Lin  
Harris Mateen  
Naiara Toker

By: /s/ Benedict Hur  
Benedict Hur

Attorneys for Defendant  
GOOGLE LLC